

Solicitando acesso ao Cisco Cloud Email Security CLI

Contents

[Introdução](#)

[Informações de Apoio](#)

[Usuários Linux e Mac](#)

[Pré-requisitos](#)

[Como faço para criar chaves RSA privadas/públicas?](#)

[Como faço para abrir uma solicitação de suporte da Cisco para fornecer minha chave pública?](#)

[Configuração](#)

[E se eu quiser me conectar a mais de um Email Security Appliance \(ESA\) ou Security Management Appliance \(SMA\)?](#)

[Como posso configurar meu ESA ou SMA para fazer login sem solicitar uma senha?](#)

[Como isso poderá ficar quando eu tiver os pré-requisitos preenchidos?](#)

[Usuários do Windows](#)

[Pré-requisitos](#)

[Como faço para criar chaves RSA privadas/públicas?](#)

[Como faço para abrir uma solicitação de suporte da Cisco para fornecer minha chave pública?](#)

[Como posso configurar meu ESA ou SMA para fazer login sem solicitar uma senha?](#)

[Configuração do PuTTY](#)

[Troubleshooting](#)

Introdução

Este documento descreve como solicitar acesso à CLI do Cloud Email Security (CES).

Informações de Apoio

Os clientes do Cisco CES têm o direito de acessar a CLI de seu ESA e SMA fornecido através de um proxy SSH usando a autenticação de chave. O acesso do CLI aos seus dispositivos hospedados deve ser limitado a indivíduos-chave dentro da sua organização.

Usuários Linux e Mac

Para clientes do Cisco CES:

Instruções para um script de shell que utiliza SSH para fazer acesso CLI via proxy CES.

Pré-requisitos

Como um cliente CES, você deve ter contratado CES On-Boarding/Ops ou Cisco TAC para que

as chaves SSH sejam trocadas e colocadas:

1. Gerar chave(s) RSA privada/pública.
2. Forneça à Cisco sua chave pública RSA.
3. Aguarde até que a Cisco salve e notifique você de que suas chaves foram salvas em sua conta de cliente CES.
4. Copie e modifique o script connect2ces.sh.

Como faço para criar chaves RSA privadas/públicas?

A Cisco recomenda o uso de 'ssh-keygen' no terminal/CLI para Unix/Linux/OS X. Use o comando `ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME>` .



Note: Para obter mais informações, visite <https://www.ssh.com/academy/ssh/keygen>.
Certifique-se de proteger o acesso às chaves privadas RSA o tempo todo.
Não envie sua chave privada para a Cisco, apenas a chave pública (.pub).
Ao enviar sua chave pública para a Cisco, identifique o endereço de e-mail/nome/sobrenome para o qual a chave se destina.

Como faço para abrir uma solicitação de suporte da Cisco para fornecer minha chave pública?

Navegue até [este](#) link.

Certifique-se de identificar corretamente o SR como "Configuração SSH/CLI do cliente do Cisco CES" e assim por diante.

Configuração

Para começar, [abra o copy do script](#) fornecido e use um desses hosts proxy para o Nome do Host.

Certifique-se de escolher o proxy correto para sua região (ou seja, se você for um cliente CES dos EUA, para acessar o data center e os dispositivos F4, use o `f4-ssh.iphmx.com`. Se você for um cliente EU CES com um dispositivo em DC alemão, use `f17-ssh.eu.iphmx.com`).

AP (`ap.iphmx.com`)
`f15-ssh.ap.iphmx.com`
`f16-ssh.ap.iphmx.com`

CA (`ca.iphmx.com`)
`f13-ssh.ca.iphmx.com`
`f14-ssh.ca.iphmx.com`

UE (`c3s2.iphmx.com`)

f10-ssh.c3s2.iphmx.com

f11-ssh.c3s2.iphmx.com

UE (eu.iphmx.com)(Alemanha DC)

f17-ssh.eu.iphmx.com

f18-ssh.eu.iphmx.com

EUA (iphmx.com)

f4-ssh.iphmx.com

f5-ssh.iphmx.com

E se eu quiser me conectar a mais de um Email Security Appliance (ESA) ou Security Management Appliance (SMA)?

Copie e salve uma segunda cópia do connect2ces.sh, como connect2ces_2.sh.



Note: Edite o 'cloud_host' para ser o dispositivo adicional que você deseja acessar. Edite 'local_port' para que seja DIFERENTE de 2222. Caso contrário, você receberá um erro, "AVISO: A IDENTIFICAÇÃO DO HOST REMOTO FOI ALTERADA!"

Como posso configurar meu ESA ou SMA para fazer login sem solicitar uma senha?

Leia [este](#) guia.

Como isso poderá ficar quando eu tiver os pré-requisitos preenchidos?

```
joe.user@my_local > ~ ./connect2ces
[-] Conectando ao servidor proxy (f4-ssh.iphmx.com)...
[-] Conexão de proxy bem-sucedida. Agora conectado a f4-ssh.iphmx.com.
[-] proxy em execução no PID: 31253
[-] Conectando ao seu dispositivo CES (esa1.rs1234-01.iphmx.com)...
```

Último login: Seg Abr 22 11:33:45 2019 a partir de 10.123.123.123
AsyncOS 12.1.0 para Cisco C100V build 071

Bem-vindo ao Cisco C100V Email Security Virtual Appliance

NOTE: Esta sessão expirará se ficar ociosa por 1.440 minutos. Qualquer alteração de configuração não confirmada será perdida. Confirme as alterações de configuração assim que elas forem feitas.

(Máquina esa1.rs1234-01.iphmx.com)>

(Máquina esa1.rs1234-01.iphmx.com)> sair

A conexão com 127.0.0.1 foi fechada.

[-] Fechando conexão proxy...

[-] Concluído.

connect2ces.sh



Observação: certifique-se de escolher o proxy correto para sua região (ou seja, se você for um cliente do CES dos EUA, para acessar o data center e os dispositivos F4, use o f4-ssh.iphmx.com. Se você for um cliente EU CES com um dispositivo em DC alemão, use f17-ssh.eu.iphmx.com.).

```
#!/bin/bash
```

```
#-- OS VALORES ABAIXO -----
```

```
# Os seguintes valores já devem ser estabelecidos com o CES:
```

```
# cloud_user="username"
```

```
# cloud_host="esaX.CUSTOMER.iphmx.com" ou "smaX.CUSTOMER.iphmx.com"
```

```
## [CERTIFIQUE-SE DE QUE VOCÊ TEM O CONJUNTO DE DATACENTERS CES REGIONAL APROPRIADO!]
```

```
# private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
```

```
# proxy_server="SERVIDOR_PROXY" [SELECIONE APENAS UM!]
```

```
#
```

```
## Para 'proxy_server', estes são proxies SSH:
```

```
##
```

```
## AP (ap.iphmx.com)
```

```
## f15-ssh.ap.iphmx.com
```

```
## f16-ssh.ap.iphmx.com
```

```
##
```

```
## CA (ca.iphmx.com)
```

```
## f13-ssh.ca.iphmx.com
```

```
## f14-ssh.ca.iphmx.com
```

```
##
```

```
## EU (c3s2.iphmx.com)
```

```
## f10-ssh.c3s2.iphmx.com
```

```
## f11-ssh.c3s2.iphmx.com
```

```
##
```

```
## EU (eu.iphmx.com)(DC alemão)
```

```
## f17-ssh.eu.iphmx.com
```

```
## f18-ssh.eu.iphmx.com
```

```
##
```

```
## EUA (iphmx.com)
```

```
## f4-ssh.iphmx.com
```

```
## f5-ssh.iphmx.com
```

```
cloud_user="nome de usuário"
```

```
cloud_host="esaX.CUSTOMER.iphmx.com"
private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
proxy_server="SERVIDOR_PROXY"
```

#-- ESSES VALORES COMO ESTÃO -----

'proxy_user' não deve mudar

'remote_port' permanece 22 (SSH)

'local_port' pode ser definido com um valor diferente, se necessário

```
proxy_user="dh-user"
```

```
remote_port=22
```

```
local_port=2222
```

#-- NÃO EDITAR ABAIXO DESTE ----- DE LINHA

```
proxycmd="ssh -f -L $local_port:$cloud_host:$remote_port -i $private_key -N
$proxy_user@$proxy_server"
```

```
printf "[-] Conectando ao seu servidor proxy ($proxy_server)...\n"
```

```
$proxycmd >/dev/null 2>&1
```

```
if nc -z 127.0.0.1 $local_port >/dev/null 2>&1; em seguida
```

```
printf "[-] Conexão de proxy bem-sucedida. Conectado ao $proxy_server.\n"
```

```
else
```

```
printf "[-] Conexão do proxy malsucedida. Saindo...\n"
```

```
sair
```

```
fi
```

Localizar processo proxy ssh

```
proxypid=`ps -xo pid,command | grep "$cloud_host" | grep "$proxy_server" | cabeça -n1 | sed "s/^[
\t]*/" | cut -d " " -f1`
```

```
printf "[-] proxy em execução no PID: $proxypid\n"
```

```
printf "[-] Conectando ao seu dispositivo CES ($cloud_host)...\n\n"
```

```
ssh -p $local_port $cloud_user@127.0.0.1
```

```
printf "[-] Fechando conexão proxy...\n"
```

```
kill $proxypid
```

```
printf "[-] Concluído.\n"
```

#-- Deseja evitar ter que digitar a senha toda vez?

#-- Consulte: <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-technote-esa-00.html>

#-- precisa de acesso a mais de um ESA ou SMA? Copie o mesmo script e renomeie para connect2ces_2.sh, ou similar.

Documento original:<https://github.com/robsherw/connect2ces>.

Usuários do Windows

Instruções para usar PuTTY e utilizar SSH para fazer acesso CLI através do proxy CES.

Pré-requisitos

Como um cliente CES, você deve ter contratado CES On-Boarding/Ops ou Cisco TAC para que as chaves SSH sejam trocadas e colocadas:

1. Gerar chave(s) RSA privada/pública.
2. Forneça à Cisco sua chave pública RSA.
3. Aguarde a Cisco para salvar e notificar você de que sua(s) chave(s) foi(ram) salva(s) em sua conta de cliente CES.
4. Configure o PuTTY conforme detalhado aqui nestas instruções.

Como faço para criar chaves RSA privadas/públicas?

A Cisco recomenda o uso do PuTTYgen (<https://www.puttygen.com/>) para Windows.

Para obter mais informações: <https://www.ssh.com/ssh/putty/windows/puttygen>.



Note: Certifique-se de proteger o acesso às chaves privadas RSA o tempo todo. Não envie sua chave privada para a Cisco, apenas a chave pública (.pub). Ao enviar sua chave pública para a Cisco, identifique o endereço de e-mail/nome/sobrenome para o qual a chave se destina.

Como faço para abrir uma solicitação de suporte da Cisco para fornecer minha chave pública?

Navegue até [este](#) link.

Certifique-se de identificar corretamente o SR como "Configuração SSH/CLI do cliente do Cisco CES" e assim por diante.

Como posso configurar meu ESA ou SMA para fazer login sem solicitar uma senha?

Leia [este](#) guia.

Configuração do PuTTY

Para começar, abra o PuTTY e use um destes hosts proxy para os Nomes de Host:

Certifique-se de escolher o proxy correto para sua região (ou seja, se você for um cliente CES

dos EUA, para acessar o data center e os dispositivos F4, use o f4-ssh.iphmx.com. Se você for um cliente EU CES com um dispositivo em DC alemão, use f17-ssh.eu.iphmx.com.).

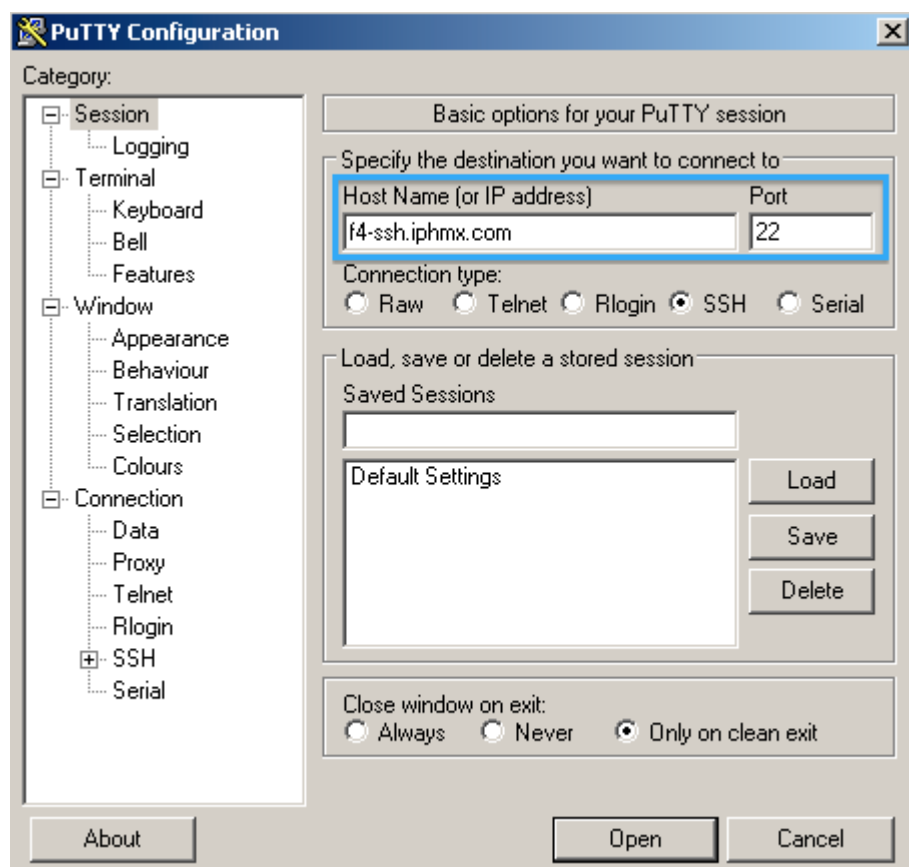
AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

CA (ca.iphmx.com)
f13-ssh.ca.iphmx.com
f14-ssh.ca.iphmx.com

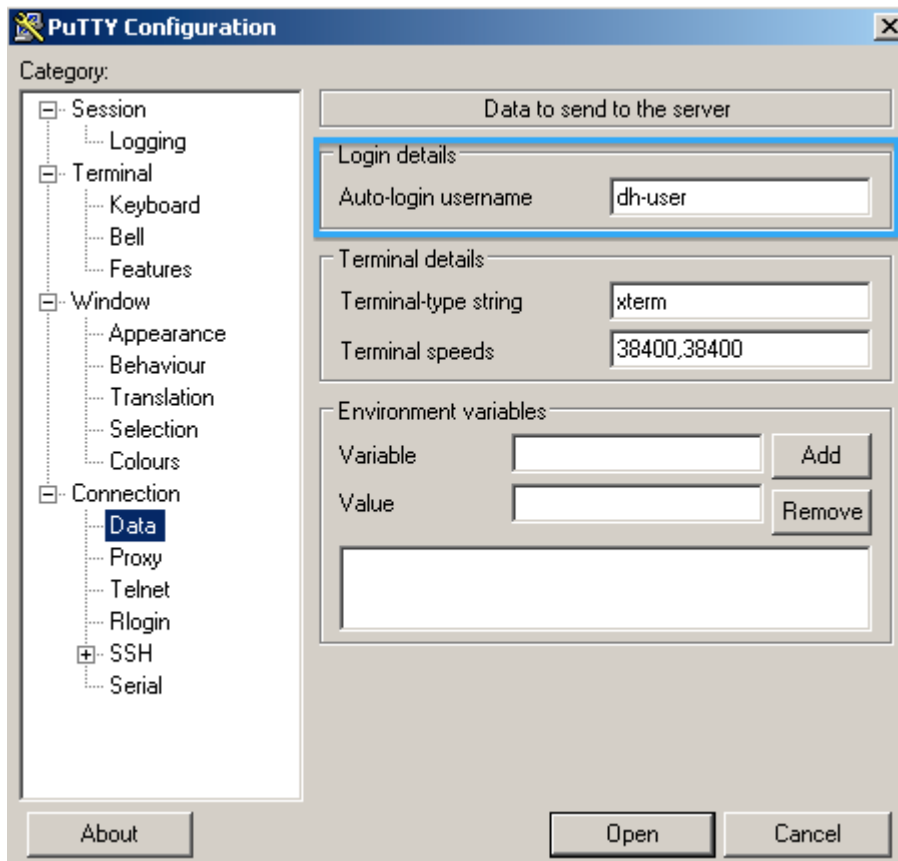
UE (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

UE (eu.iphmx.com)(Alemanha DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

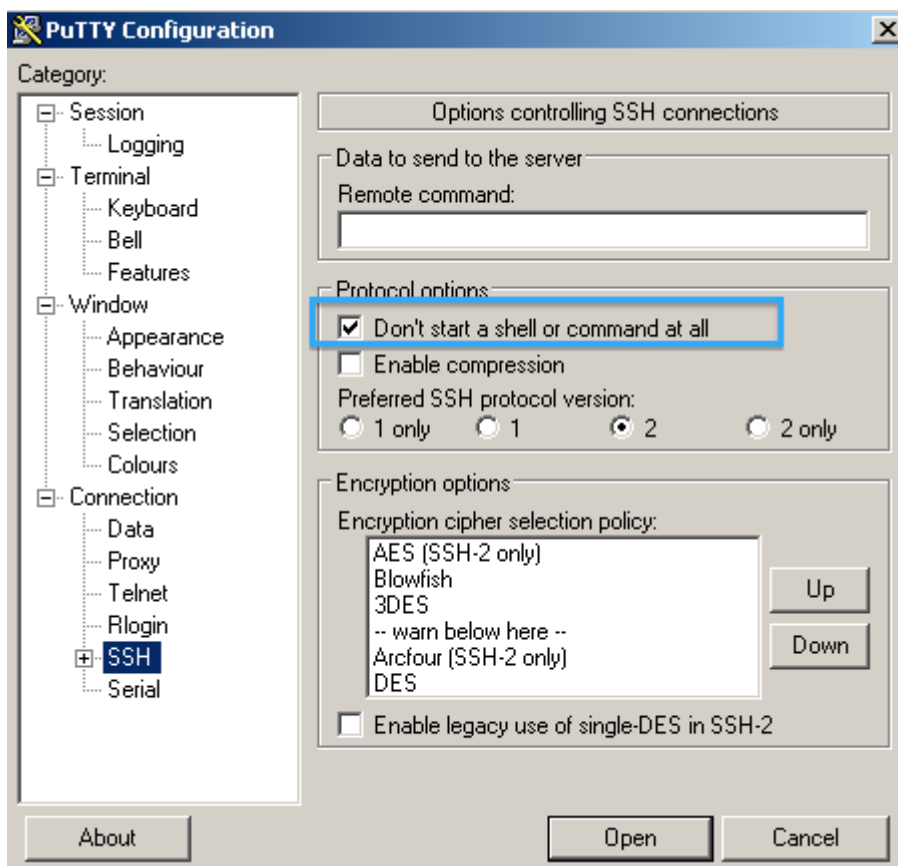
EUA (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



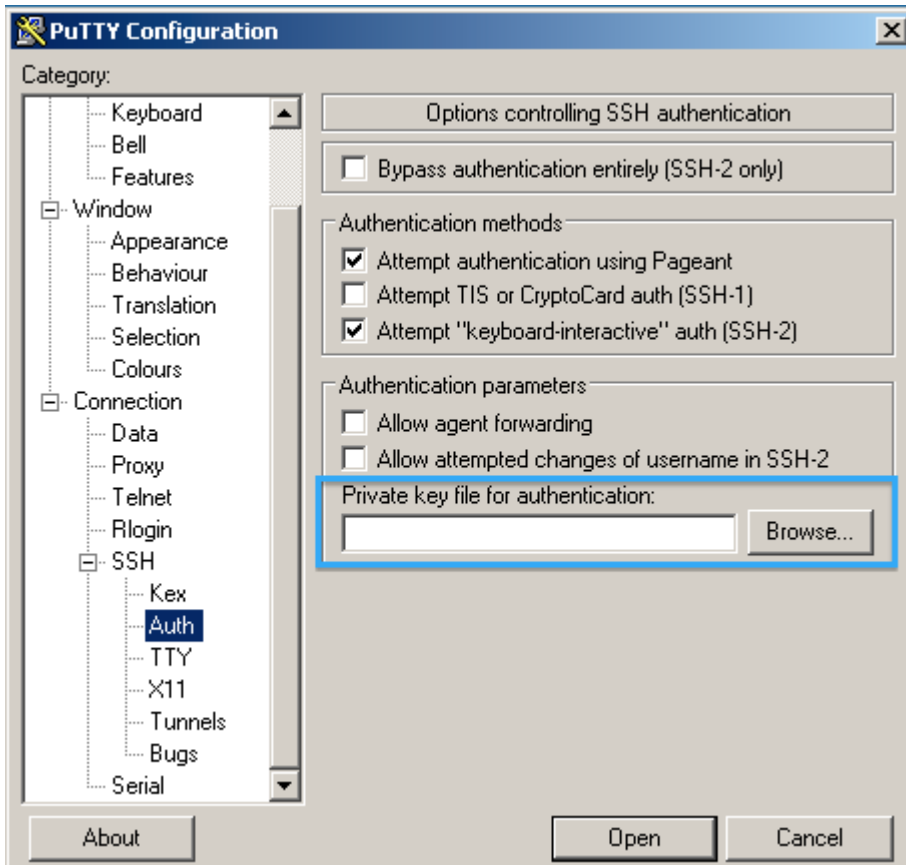
Clique em Dados e, para obter detalhes de login, use o nome de usuário de login automático e digite dh-user.



Escolha SSH e marque Não iniciar um shell ou comando.



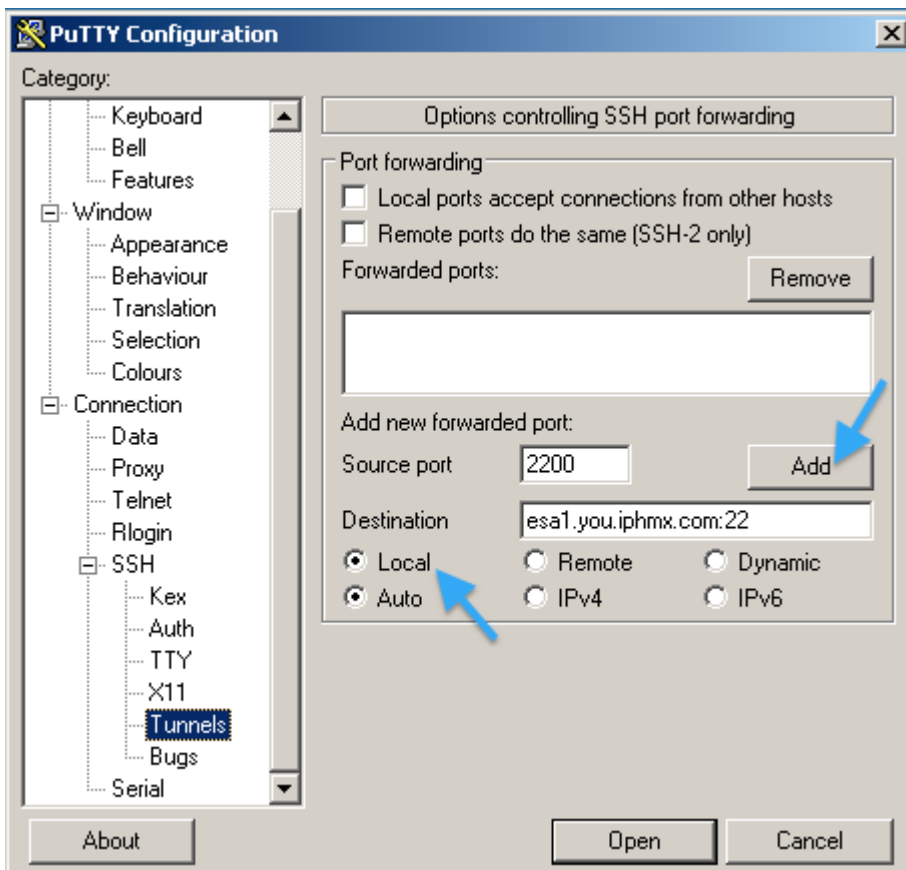
Clique em Autand para arquivo de chave privada para autenticação, navegue e escolha sua chave privada.



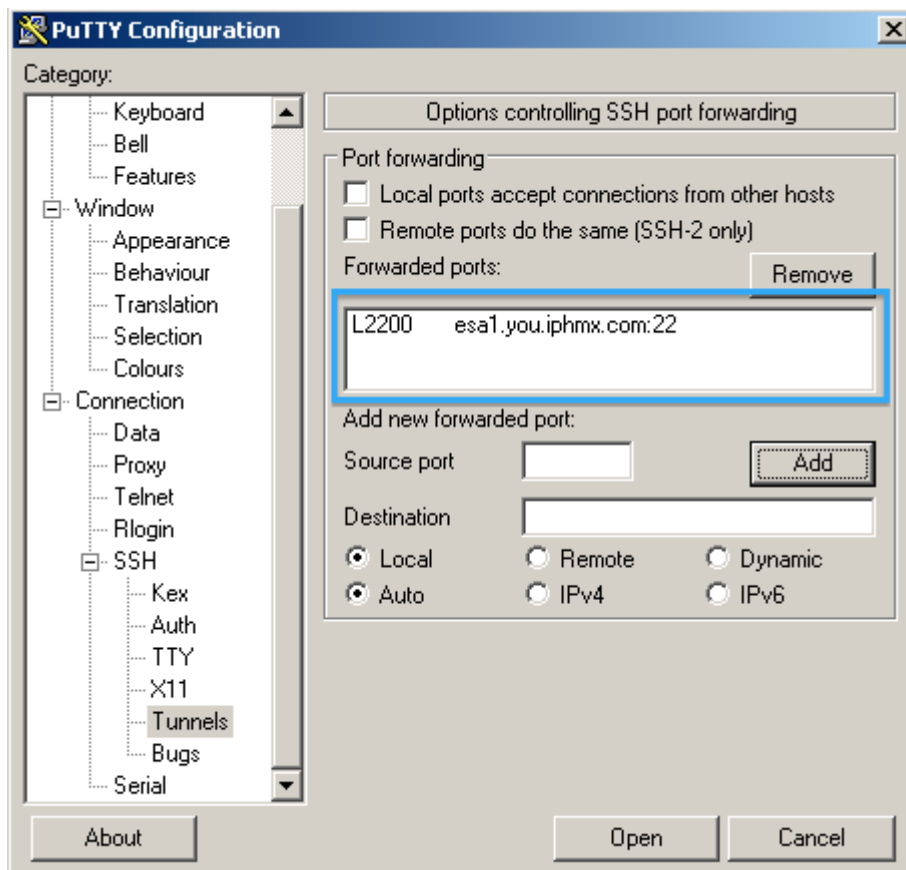
Clique em Tunnels.

Insira em uma porta de origem; essa é qualquer porta arbitrária de sua escolha (o exemplo usa 2200).

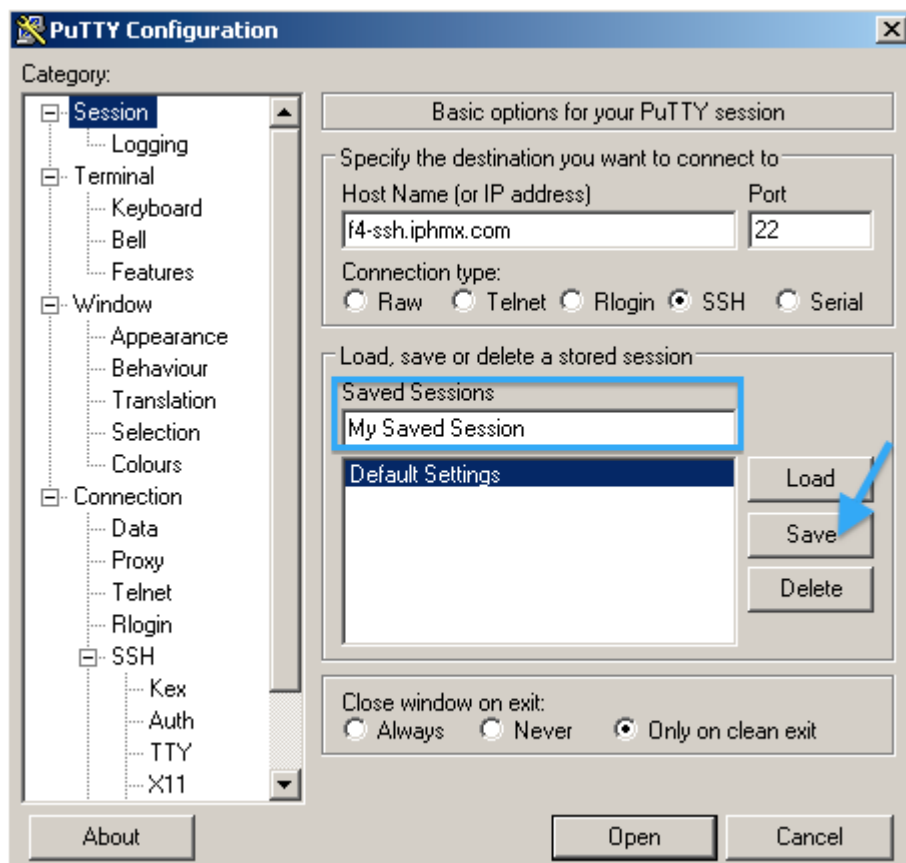
Insira em aDestination; esse é o seu ESA ou SMA + 22 (especificando a conexão SSH).



Depois de clicar em Adicionar, ele deverá ter a seguinte aparência.



Para salvar a sessão para uso futuro, clique em Sessão. Insira um nome para a 'Sessão salva' e clique em Salvar.



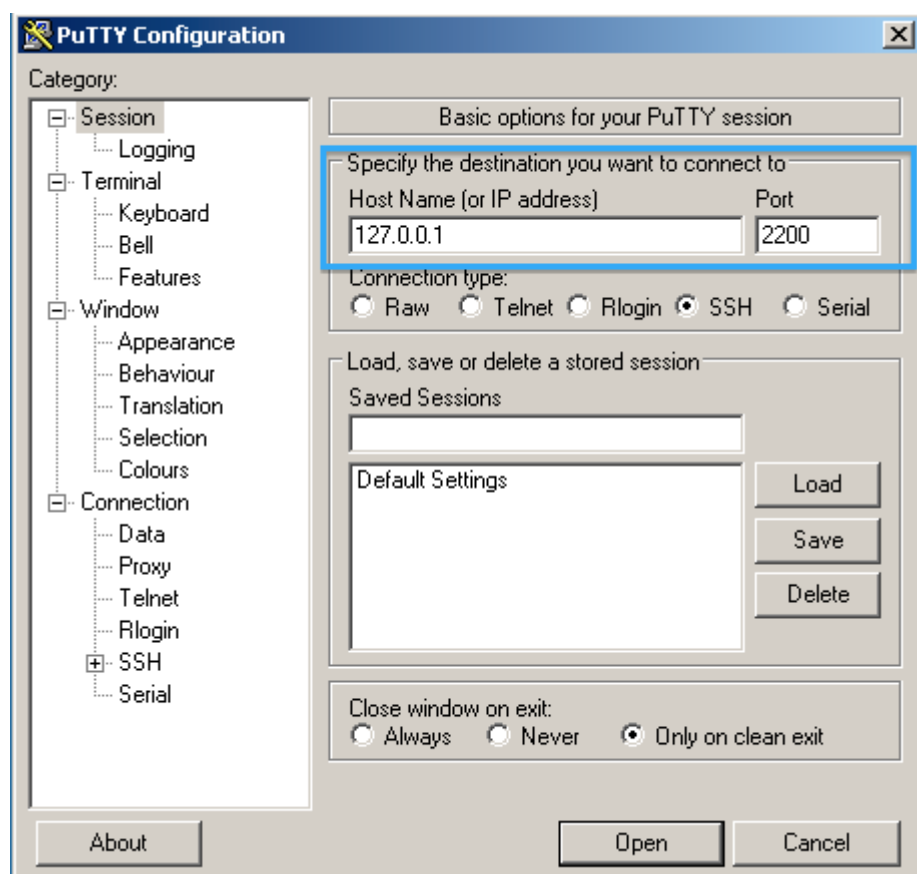
Neste momento, você pode clicar em Abrir e iniciar a sessão proxy.

Não haverá nenhum login ou prompt de comando. Agora você precisará abrir uma segunda sessão PuTTY para seu ESA ou SMA.

Use o nome de host 127.0.0.1 e use o número da porta origem na configuração de túnel mostrada anteriormente.

Este exemplo usa 2200.

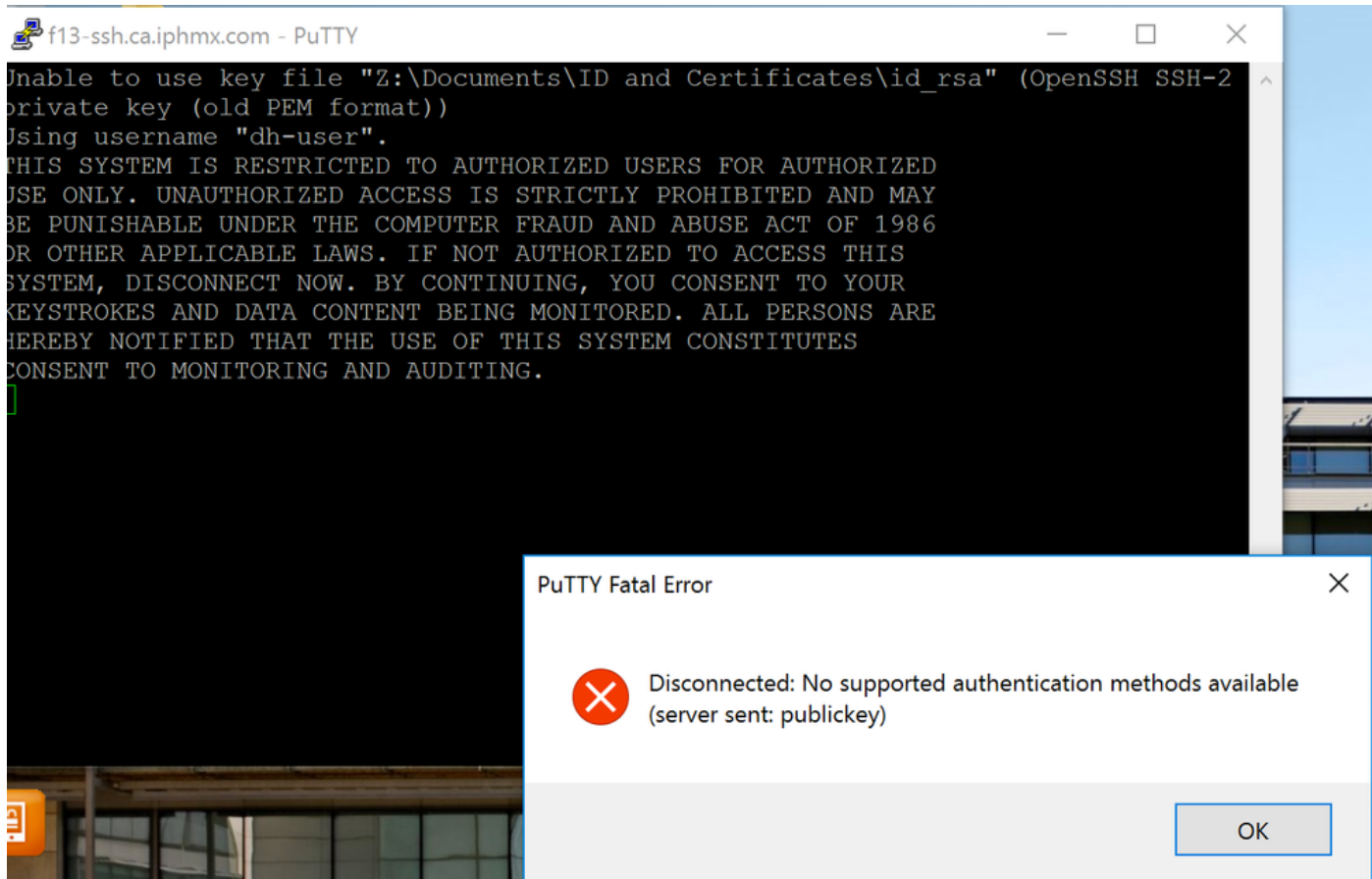
Clique em Abrir para se conectar ao seu equipamento.



Quando solicitado, use o nome de usuário e a senha do equipamento, da mesma forma que usará com o acesso à interface do usuário.

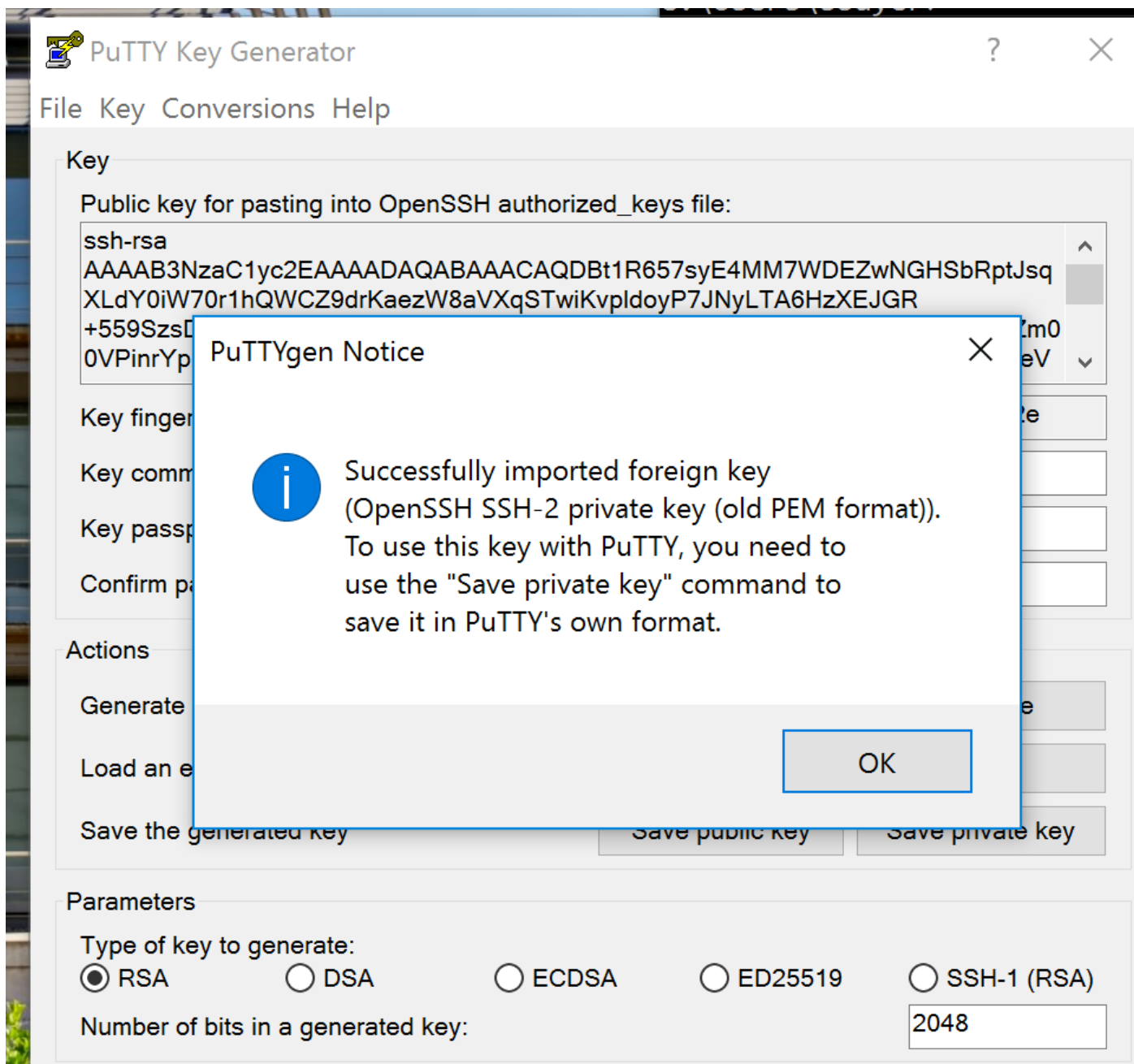
Troubleshooting

Se o seu par de chaves SSH foi gerado usando o OpenSSH (não PuTTY), você não poderá se conectar e será apresentado um erro de "formato PEM antigo".



A chave privada pode ser convertida [usando o Gerador de chave PuTTY](#).

- Abra o Gerador de chave PuTTY.
- Clique em Carregar para procurar e carregar sua chave privada existente.
- Você precisará clicar na lista suspensa e escolher Todos os arquivos (.) para poder localizar a chave privada.
- Clique em Abrir depois de localizar sua chave privada.
- Puttygen fornecerá um aviso como nesta imagem.



- Clique em Salvar chave privada.
- Em sua sessão PuTTY, use essa chave privada convertida e salve a sessão.
- Tente reconectar-se com a chave privada convertida.

Confirme se você pode acessar seus equipamentos por meio da linha de comando.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.